Research Paper

Huntsman Security

The Cyber Security Malware Crisis is Deepening

Huntsman®

Defence-Grade Cyber Security

Huntsman Security research finds malware crisis is deepening for security teams and businesses

Background

The cyber security threat landscape means that businesses are increasingly having to detect attacks from inside and outside the organisation in real-time as they deal with the wide variety of alerts and reports from their extensive array of security solutions that each focus on specific attack types.

Detected threats, both real and false, must be verified and correlated with threat intelligence and other contextual information to categorise and prioritise them for further analysis and resolution.

Huntsman Security conducted the research presented below into this, often manual, process to reveal the scale of problems security analysts, and their businesses, are facing with regard to malware attacks - typically the commonest category of cyber threat encompassing phishing, advanced persistent threats, viruses or ransomware.

The results confirmed our views that this problem is one that is continuing to grow. In the sections below we discuss the technology, process and people aspects of this problem.

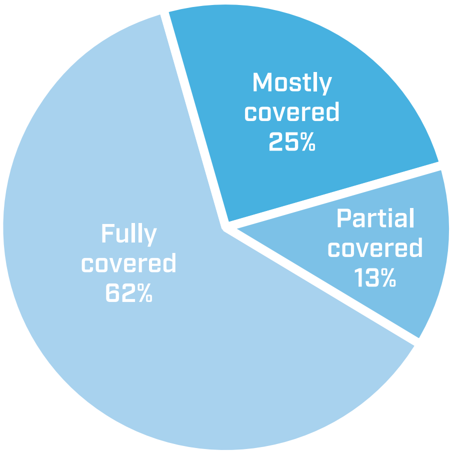
Malware Detection

The first line of defence against malware is the ability to detect it arriving. As the number of attack vectors has grown to include email, attachments, drive-by downloads, compromised web pages and social media content so has the sophistication of phishing, spear phishing, whaling and watering-hole attacks.

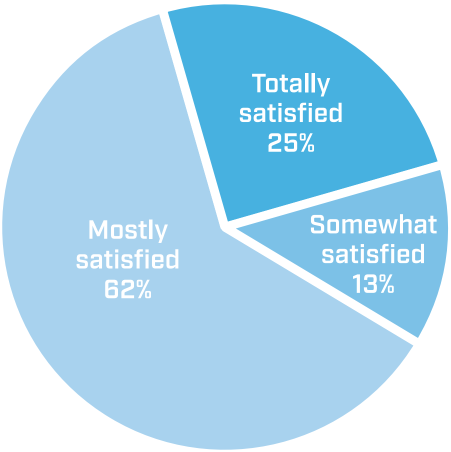
Despite malware being a high-profile, well publicised threat, our research found that over a third of organisations are not fully detecting malware, with almost 15% only detecting it partially.

These deficits in detection highlight significant gaps in the defence coverage and capabilities of businesses – clearly attackers and malware writers are continuing to find ways in. The current approach is only a partial success.

Detection Coverage



Satisfaction with technology



This shortfall is not down to lack of effort. The survey also asked respondents about common controls that were deployed and found that 9 out of 10 companies are managing multiple solutions from multiple vendors to deliver the level of protection they have achieved. This diversity of solutions brings its own challenges in managing and correlating information across several silos.

Rather worryingly survey responses indicated that only a quarter of companies are completely happy with their malware detection technologies.

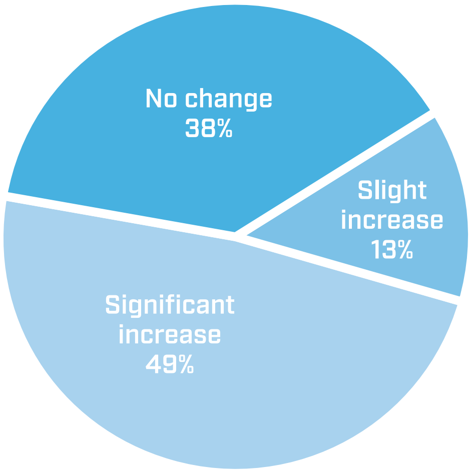
It is easy to conclude that improved levels of protection will result in an increasing detection rate as new threats and families of attack emerge and the solutions evolve to uncover them. This will in turn lead to a further increased workload for security analysts.

A Growing Technology Problem

Anecdotally the risks from malware are increasing. New trends like the increase in ransomware (like the recent WannaCry attack) are apparent and attract significant attention. However, for companies and security teams at the coal-face it is right to ask whether the reality matches the headlines.

Huntsman's survey found that the observed rate and prevalence of these attacks is indeed a growing problem.

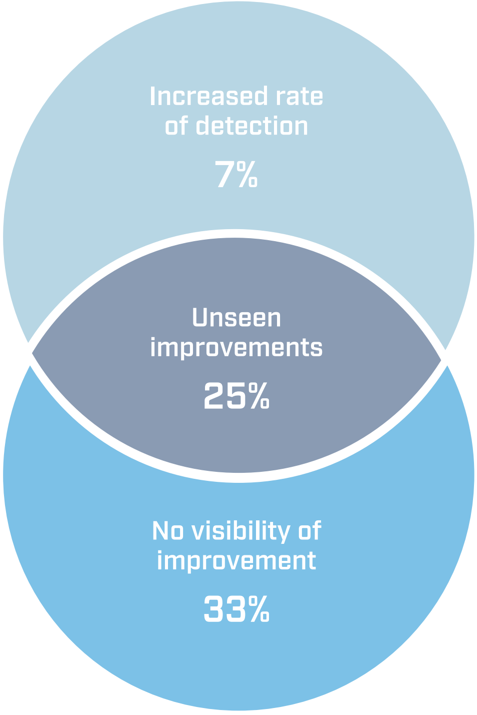
Reported Malware Volumes



None of the companies surveyed reported a decrease in malware cases or detections. Overall two thirds saw increases and half reported this increase was significant.

The companies (almost 40% of respondents) who reported the trend being flat gave several interesting reasons behind this observation. The explanations given were:

- More malware was reported as being blocked
- There was better management of vulnerabilities
- Improved staff awareness



The Business View

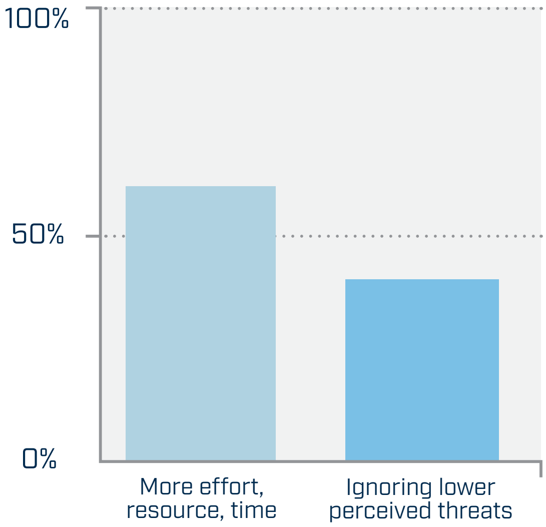
Outside of the security operations function, the management perception of the scale of the risk and the effectiveness of the security processes reveals a complex picture. The survey sought to understand how visible the problem or outcomes were to the wider business and stakeholders outside of the security team and hence away from the coal-face.

Of the companies that reported an increased volume of malware detection, around 40% (a quarter of all respondents in total) had no perception within the business of the efforts that were underway. In terms of outcomes or results, despite the increases in effort, only 10% of companies reported a visible reduction in malware incidents, and a third reported little or no improvement.

These perceptions may sap the enthusiasm of those working hard to counter the malware threat. Furthermore, the survey found that a third of companies don't even report malware threat statistics at management level.

This flow of information, where it exists, is clearly a weak link in the reporting chain – responses show that a quarter of companies admit business stakeholders are not getting adequate information about malware incidents.

How are teams dealing with the increased threat?



Security Operations Processes

For those businesses dealing with an increase in malware volumes, and given the well publicised skills shortages in cyber security; the survey asked how they were coping with the higher workload and incidences of malware within the security operations function.

The responses show that around 60% of companies are having to apply more effort, resource and time to investigate the malware reports they are receiving from their detection systems - i.e. they are having to work harder.

More worryingly, 40% reported that they are dealing with the increase by simply ignoring lower perceived threats in order to address the most critical ones.

We can conclude that in many cases the processes being followed provide an incomplete, subjective and possibly inconsistent outcome. This is therefore likely to result in some serious cases slipping through the net.

Security Outcomes

The final survey questions probed the outcomes and perceived value of the increased investment in controls, the continually increasing efforts and the management attention.

A key measure of the success of cyber security processes is how long it takes for an attack to be detected, understood, contained and resolved or removed. This is referred to as the "time at risk" or the "dwell time".

Only half of companies report that they are consistently tracking how long they are at risk before a given malware infection is resolved. This inability or failure to measure and report on what should be a key performance indicator means that accurate conclusions about risk exposure are difficult to formulate.

Accepted wisdom is that the longer an attacker is able to spread from an initial foothold or to extract data the greater the impact of the incident. It is widely reported that embarrassment and regulatory sanctions are greater where attacks have been undetected or unresolved for extended periods of time.

Despite the efforts and attention that malware is receiving in terms of investment in detection solutions, increased security operations effort and management reporting, only 25% of companies reported that their *time at risk* was reducing in the face of this threat.

Forrester Research Viewpoint ...

> "Alert volumes are increasing every year ... security leaders need to dig their teams out from under the alert deluge, and this necessitates sophisticated analytics and mature workflows executed via automation."

Forrester Research, TechRadar:
Zero Trust Network Threat Mitigation
Technologies, Q4 2016.

Conclusions

The research confirmed the hypothesis that malware is a problem that is not only growing, but that it is doing so at a rate that businesses are struggling to deal with.

Whether it is the volume of alerts, the complexity of understanding the extent of an infection or the need to provide meaningful reports to business stakeholders – the efforts of security teams risk being overwhelmed.

For business stakeholders, the visibility and benefits from the continued investment in technical security controls and an ever-growing demand for additional skilled resources are proving elusive.

"More of the same" is unlikely to be a viable strategy to redress this. The need for greater automation and intelligence in technical monitoring and operations is clear.

Automation of the threat verification and resolution processes will reduce the overall workload by rapidly processing alerts and reports to determine which are serious and need attention or which are benign, routine or unimportant.

Enabling analysts to understand the threats they are presented with, giving them context and intelligent answers to diagnostic questions, improves decision-making and enables a quick, accurate and consistent result to be achieved.

Focussing security teams on threats that really matter instead of swamping them with background noise, will give them more time for improving overall cyber security hygiene.

This will provide several benefits as it will:

- Unlock teams' abilities to provide more meaningful, timely and accurate reports to board-level stakeholders.
- Allow them to take a more proactive stance on emerging threats.
- Provide the business with a clearer and more positive view of improving security outcomes.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC
t: **+61 2 9419 3200**
e: **info@huntsmansecurity.com**
Level 2, 11 Help Street
Chatswood NSW 2067

EMEA
t: **+44 845 222 2010**
e: **ukinfo@huntsmansecurity.com**
7-10 Adam Street, Strand
London WC2N 6AA

NORTH ASIA
t: **+81 3 5809 3188**
e: **info@huntsmansecurity.com**
TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

AMERICAS
toll free: **1-415-655-6807**
e: **usinfo@huntsmansecurity.com**
Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman